Architettura di base Routed Bridged Encapsulation

Sommario

Introduzione
Presupposto
Tecnologie in breve
Descrizione operativa
Vantaggi RBE
Considerazioni sull'implementazione
Architettura di rete
Considerazioni di progettazione per l'architettura RBE
Punti chiave della soluzione RBE
CPE
Gestione IP
Come raggiungere una destinazione di servizio
Accesso a Internet
Servizi all'ingrosso
Accesso aziendale
Funzionalità di selezione dei servizi
Conclusioni
Informazioni correlate

Introduzione

Questo documento descrive un'architettura ADSL (Asymmetric Digital Subscriber Line) end-to-end che utilizza la funzionalità Routed Bridged Encapsulation (RBE) per Cisco 6400 Universal Access Concentrator (UAC). La tecnologia RBE è stata sviluppata per risolvere i problemi noti del bridging RFC1483, tra cui le tempeste di trasmissione e la sicurezza. Ad eccezione del fatto che opera esclusivamente su ATM, la funzione RBE funziona in modo identico a half-bridging. È possibile ottenere ulteriori livelli di scalabilità, prestazioni e sicurezza utilizzando le caratteristiche esclusive degli abbonati xDSL.

Presupposto

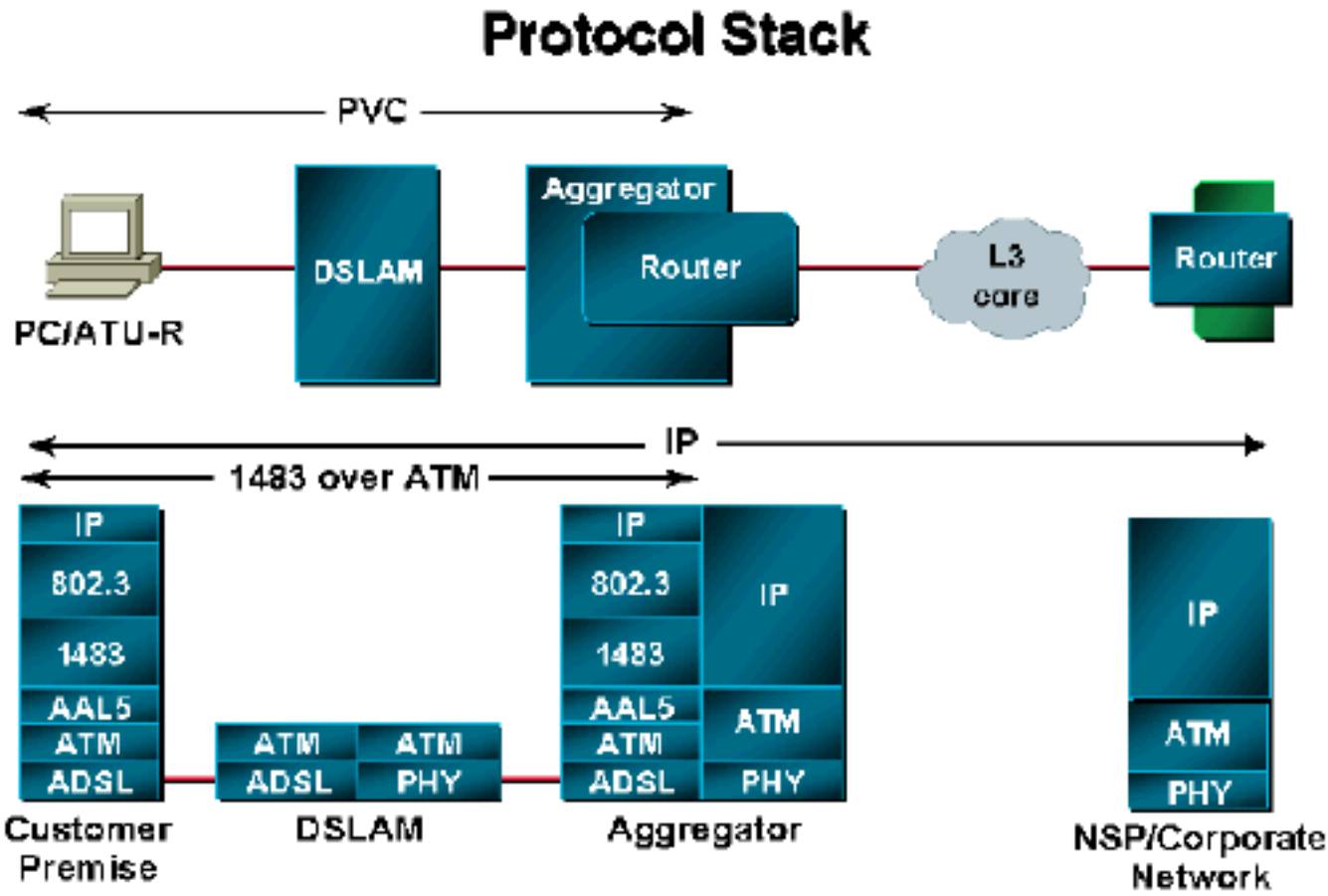
L'architettura di base è progettata utilizzando il modello dell'architettura di riferimento del forum ADSL. L'architettura copre diverse offerte di servizi da parte del provider di accesso alla rete e diversi scenari di inoltro del traffico degli utenti al provider di servizi di rete (NSP). In questa architettura, l'RBE è il metodo di incapsulamento usato da Cisco 6400. Il contenuto di questo documento si basa sulle distribuzioni esistenti, nonché su alcuni test interni eseguiti sull'architettura. Per caratteristiche avanzate e modifiche, consultare le note sulla versione

dell'ultima versione del software Cisco IOS®. Attualmente, la funzionalità RBE è supportata sulle piattaforme Cisco 6400, Cisco 7200 e Cisco 7500. Questo documento riguarda solo le discussioni su Cisco 6400.

Tecnologie in breve

Dal punto di vista della rete, la connessione ATM sembra una connessione instradata. Il traffico di dati viene ricevuto come pacchetti RFC1483, ma si tratta di frame RFC1483 Ethernet o IEEE 802.3. Anziché eseguire il bridging del frame Ethernet o IEEE 802.3, come nel caso del bridging RFC1483 standard, il router esegue il routing sull'intestazione di layer 3. Ad eccezione di alcuni controlli di corsivo, l'intestazione bridge viene ignorata. Questa condizione viene spiegata in dettaglio nella sezione successiva.

Descrizione operativa



Da un punto di vista operativo, il router funziona come se l'interfaccia del bridge di routing fosse collegata a una LAN Ethernet. L'operazione è descritta di seguito in due modi: i pacchetti provenienti dai locali del cliente e i pacchetti destinati ai locali del cliente.

Per i pacchetti provenienti dalla sede del cliente, l'intestazione Ethernet viene saltata e l'indirizzo IP di destinazione viene esaminato. Se l'indirizzo IP di destinazione è nella cache route, il pacchetto viene commutato rapidamente all'interfaccia in uscita. Se l'indirizzo IP di destinazione non è presente nella cache route, il pacchetto viene accodato per la commutazione del processo. In modalità process switch, per individuare l'interfaccia in uscita attraverso cui deve essere indirizzato il pacchetto, consultare la tabella di routing. Dopo aver identificato l'interfaccia in uscita, il pacchetto viene instradato attraverso quell'interfaccia. Ciò si verifica senza la necessità di un gruppo di bridge o di un'interfaccia virtuale del gruppo di bridge (BVI).

Per i pacchetti destinati all'abitazione del cliente, l'indirizzo IP di destinazione del pacchetto viene esaminato per primo. L'interfaccia di destinazione viene determinata dalla tabella di routing IP. Successivamente, il router controlla la tabella ARP (Address Resolution Protocol) associata all'interfaccia per verificare se un indirizzo MAC di destinazione deve essere inserito nell'intestazione Ethernet. Se non viene trovato alcun indirizzo, il router genera una richiesta ARP per l'indirizzo IP di destinazione. La richiesta ARP viene inoltrata solo all'interfaccia di destinazione. Ciò è in contrasto con il bridging, in cui la richiesta ARP viene inviata a tutte le interfacce del gruppo bridge.

Per uno scenario in cui vengono utilizzate interfacce senza numero (in cui è possibile trovare due sottoscrittori nella stessa subnet), l'interfaccia del bridge indirizzato utilizza il proxy ARP. Ad esempio, 192.168.1.2 (host A) desidera comunicare con 192.168.1.3 (host B). Tuttavia, l'host A si trova nella stessa subnet dell'host B.

L'host A deve imparare l'indirizzo MAC dell'host B inviando una trasmissione ARP all'host B. Quando l'interfaccia bridge di routing sul dispositivo di aggregazione riceve la trasmissione, invia una risposta ARP proxy con l'indirizzo MAC 192.168.1.1, host A. Prende l'indirizzo MAC, lo inserisce nella sua intestazione Ethernet e invia il pacchetto. Quando il router riceve il pacchetto, scarta l'intestazione e cerca l'indirizzo IP di destinazione, quindi lo instrada sull'interfaccia corretta.

Vantaggi RBE

La tecnologia RBE è stata sviluppata con l'intento di risolvere alcuni dei problemi che l'architettura di bridging RFC1483 deve affrontare. RBE conserva i principali vantaggi dell'architettura di bridging RFC1483, eliminando la maggior parte degli inconvenienti.

- Configurazione minima delle apparecchiature presso la sede del cliente (CPE).Il fornitore di servizi lo considera importante in quanto non richiede più un gran numero di rulli compressi e non deve più investire ingenti risorse di personale per il supporto di protocolli di livello superiore. Il CPE in modalità bridge funziona come un dispositivo molto semplice. Il CPE richiede una risoluzione minima dei problemi, in quanto tutto ciò che proviene da Ethernet passa direttamente al lato WAN.
- Migrazione semplice da architetture di bridging pure a RBE. Nessuna modifica richiesta al destinatario predefinito.
- Evita i problemi di dirottamento IP e di spoofing ARP che si verificano nelle architetture tradizionali con bridging puro. La tecnologia RBE evita inoltre i temporali nelle trasmissioni utilizzando connessioni point-to-point. La sicurezza è il principale svantaggio delle architetture puramente "bridging".
- Rispetto alle architetture di bridging puro, RBE offre prestazioni superiori grazie all'implementazione del routing sul dispositivo di aggregazione. Inoltre, la funzionalità RBE è più scalabile in quanto non presenta limitazioni per i gruppi di bridge.
- Supporta la selezione Web di layer 3 tramite Cisco Service Selection Gateway (SSG).

Considerazioni sull'implementazione

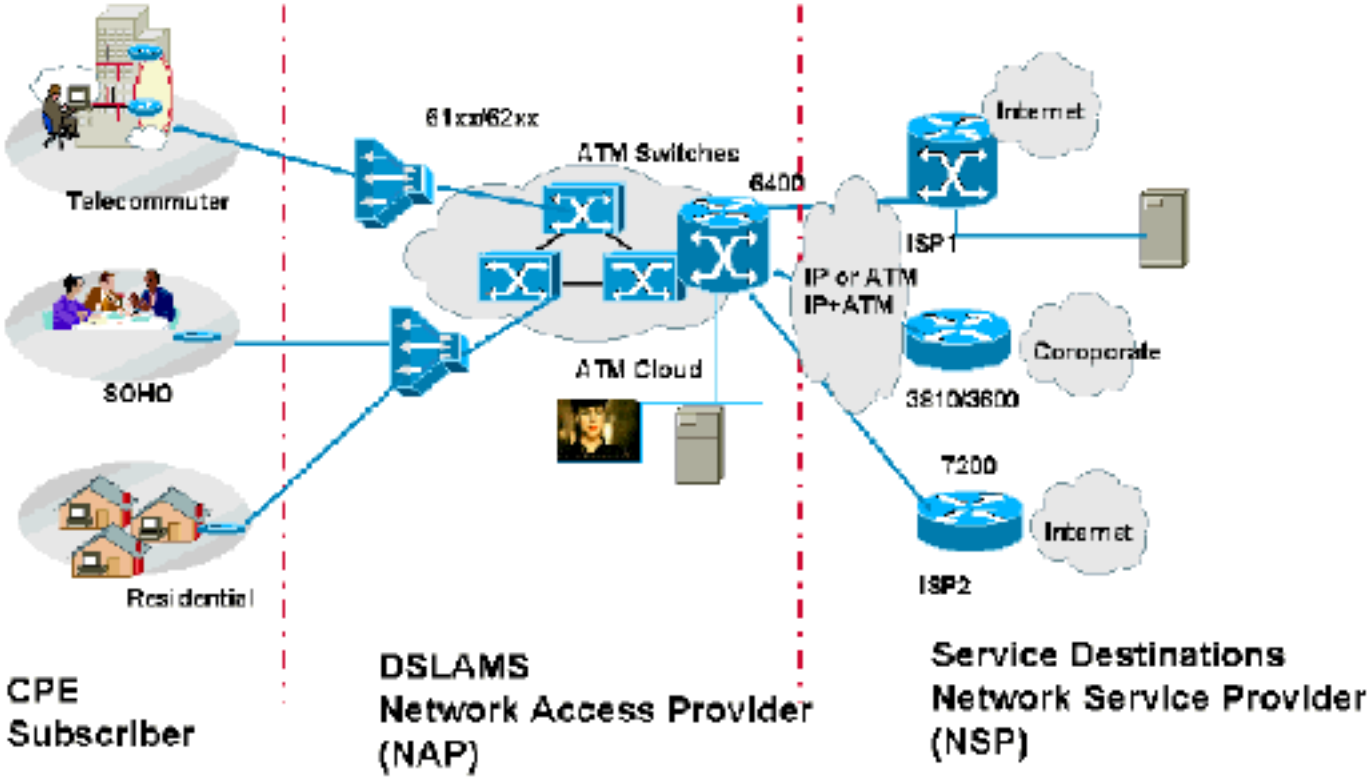
Alcuni dei punti chiave da considerare prima di implementare questa architettura sono gli stessi indicati nel documento RFC1483 Bridging Baseline Architecture.

La funzione RBE è consigliata quando:

- Gli scenari sono gli stessi delle architetture di bridging esistenti.
- Protezione accesso alla rete desidera eseguire solo una gestione minima dei CPE. Il concetto di CPE semplice richiede una configurazione minima o nulla dopo l'implementazione del CPE nella posizione del destinatario predefinito.
- Protezione accesso alla rete non desidera installare e gestire client host sugli host dietro CPE con bridging. Queste attività di installazione e manutenzione aumentano i costi di installazione e manutenzione, inclusa la fornitura di personale dell'help desk con conoscenza del software client e del sistema operativo su cui il client è in esecuzione.
- Protezione accesso alla rete desidera distribuire una rete con bridging scalabile e protetta utilizzando CPE *esistenti* (che possono funzionare solo in modalità bridging RFC1483) e desidera offrire funzionalità di selezione dei servizi.

La prossima discussione spiega come l'architettura RBE si adatta e si adatta a diversi modelli di business.

Architettura di rete



L'architettura di rete RBE è simile all'architettura di bridging RFC1483. Come specificato in tale architettura, il dispositivo di aggregazione potrebbe trovarsi in Protezione accesso alla rete o nell'NSP. Se si utilizza un'architettura end-to-end del PVC (Permanent Virtual Circuit), l'NSP termina gli utenti e configura l'RBE sul dispositivo di aggregazione. Se Protezione accesso alla rete preferisce fornire servizi all'ingrosso più la selezione dei servizi, può scegliere di terminare tali abbonati e ottenere indirizzi IP da un server DHCP (Dynamic Host Configuration Protocol) locale. Nel caso dei servizi all'ingrosso, il NAP può scegliere di ottenere gli indirizzi IP dall'NSP. Questi scenari sono illustrati in dettaglio nella sezione Gestione IP in questo documento.

Considerazioni di progettazione per l'architettura RBE

RBE elimina i principali rischi per la sicurezza associati all'architettura di bridging RFC1483.

Inoltre, la tecnologia RBE offre prestazioni migliori ed è più scalabile in quanto le sottointerfacce vengono trattate come interfacce di routing.

In questa sezione vengono illustrati alcuni dei punti chiave da tenere in considerazione prima di progettare l'architettura RBE. Per il lato sottoscrittore, i principi di progettazione rimangono gli stessi dell'architettura di bridging RFC1483.

In RBE, a un singolo circuito virtuale (VC) viene assegnata una route, un set di route o una subnet CIDR (Classless Interdomain Routing). In questo modo, l'ambiente di fiducia viene ridotto solo alla singola sede del cliente rappresentata dagli indirizzi IP nel set di route o dal blocco CIDR. L'ISP controlla inoltre gli indirizzi assegnati all'utente. A tale scopo, è necessario configurare una subnet nell'interfaccia utente. Pertanto, se un utente configura in modo errato le apparecchiature con un indirizzo IP esterno all'intervallo di indirizzi allocato (probabilmente causando il flusso dei pacchetti ARP fino al router), il router genera un errore di "cavo errato" e rifiuta di immettere il mapping errato di indirizzi IP-MAC nella relativa tabella ARP.

È possibile distribuire RBE utilizzando solo sottointerfacce ATM point-to-point. Non può essere distribuito su sottointerfacce multipoint. Anche se il lato sottoscrittore è collegato, non è necessario definire gruppi bridge o interfacce BVI perché le sottointerfacce vengono trattate come interfacce indirizzate.

Le sottointerfacce point-to-point ATM possono essere numerate o non numerate ad altre interfacce.

Per definizione, un'interfaccia numerata è un'interfaccia a cui è assegnato un indirizzo IP specifico con una subnet mask fissa. Ad esempio:

```
Interface atm0/0/0.132 point-to-point
ip address 192.168.1.1 255.255.255.252
```

Come mostrato nell'esempio, quando si distribuisce la funzionalità RBE con un'interfaccia numerata, è necessario che vi sia una subnet distinta per ogni sottoscrittore. L'host all'estremità del sottoscrittore deve essere configurato per 192.168.1.2. All'estremità del sottoscrittore è presente un solo host. Se il requisito è quello di supportare più host, la subnet mask scelta deve supportare più host.

Le interfacce numerate consentono a Protezione accesso alla rete di controllare il numero di host connessi dal sottoscrittore dietro CPE. Come spiegato in precedenza, questa mancanza di controllo è stato un problema importante nell'architettura di bridging RFC1483.

Tuttavia, questa metodologia utilizza troppi indirizzi IP. Sarà necessario allocare una subnet per sottoscrittore, utilizzare un indirizzo IP per l'interfaccia secondaria ATM e lasciare inutilizzati l'indirizzo di broadcast e tutti gli indirizzi zero. Pertanto, per avere un host dietro CPE, è necessario definire almeno una subnet mask di 255.255.255.252. Tenuto conto della scarsità di indirizzi IP, questa opzione potrebbe non essere praticabile a meno che Protezione accesso alla rete/Server dei criteri di rete non utilizzi lo spazio degli indirizzi privato e non esegua Network Address Translation (NAT) per raggiungere il mondo esterno.

Per conservare gli indirizzi IP, un'alternativa sarebbe utilizzare interfacce senza numero. Per definizione, un'interfaccia senza numero è un'interfaccia che utilizza l'indirizzo IP di un'altra interfaccia con il comando **ip unnumber**. Ad esempio:

```
!
interface loopback 0
ip address 192.168.1.1 255.255.255.0
!
interface atm0/0/0.132 point-to-point
ip unnumbered loopback 0
!
interface atm0/0/0.133 point-to-point
ip unnumbered loopback 0
```

Come mostrato nell'esempio, un indirizzo IP e una subnet vengono applicati solo all'interfaccia di loopback. Tutte le sottointerfacce ATM vengono numerate in base all'interfaccia di loopback. In questo scenario, tutti i sottoscrittori terminati su interfacce ATM (senza numero per il loopback 0) si troverebbero sulla stessa subnet di quello del loopback 0. Ciò implica che i sottoscrittori si troverebbero sulla stessa subnet, ma che potrebbero accedere tramite interfacce con routing diverse. In questa situazione, per il router diventa un problema identificare il sottoscrittore dietro cui si trova l'interfaccia ATM. Per Cisco IOS, la versione 192.168.1.0 (nel diagramma di gestione IP) è collegata direttamente tramite il loopback di interfaccia 0 e non invia mai il traffico destinato a nessuno degli indirizzi host della subnet tramite altre interfacce. Per risolvere questo problema, è necessario configurare in modo esplicito le route host statiche. Ad esempio:

```
ip route 192.168.1.2 255.255.255.255 atm0/0/0.132
ip route 192.168.1.3 255.255.255.255 atm0/0/0.133
```

Come specificato nell'esempio, quando il router deve prendere una decisione di routing e inoltrare il traffico destinato a 192.168.1.2, sceglierà ATM 0/0/0.132 come interfaccia in uscita e così via. Senza specificare le route host statiche, il router sceglie l'interfaccia in uscita come loopback 0 e scarta il pacchetto.

Anche se l'interfaccia senza numero conserva gli indirizzi IP, richiede un'ulteriore attività di configurazione delle route host statiche sul Node Route Processor (NRP) per ciascun sottoscrittore. Si noti che se un sottoscrittore ha, ad esempio, 14 host dietro il CPE, non è necessario disporre di route host statiche per ciascun host. È possibile definire un percorso riepilogativo per l'interfaccia secondaria ATM.

Finora, questa spiegazione ha presupposto che gli host dietro il CPE saranno configurati per indirizzi IP statici. Questa supposizione non è vera nei progetti reali. Nella pratica, Protezione accesso alla rete desidera eseguire operazioni minime di configurazione e manutenzione per il CPE e gli host collegati. A tale scopo, gli host devono ottenere i propri indirizzi in modo dinamico utilizzando un server DHCP.

Per ottenere dinamicamente i relativi indirizzi IP, gli host devono essere configurati in modo da ottenere gli indirizzi IP da un server DHCP. All'avvio, l'host invia le richieste DHCP. Queste richieste vengono quindi inoltrate al server DHCP appropriato, che assegna all'host un indirizzo IP da uno degli ambiti definiti in precedenza.

Per inoltrare le richieste DHCP iniziali dall'host al server DHCP appropriato, è necessario applicare il comando **ip helper-address** all'interfaccia che riceve i broadcast. Dopo aver ricevuto i broadcast, Cisco IOS controlla la configurazione dell'indirizzo dell'helper IP per l'interfaccia e inoltra le richieste in un pacchetto unicast al server DHCP appropriato il cui indirizzo IP è specificato in indirizzo dell'helper IP. Dopo aver risposto con l'indirizzo IP, il server DHCP invia la risposta all'interfaccia sul router che ha originariamente inoltrato la richiesta. Viene utilizzata come interfaccia in uscita per inviare la risposta del server DHCP all'host che ha richiesto originariamente il servizio. Il router installa inoltre automaticamente un percorso host per questo indirizzo.

Se RBE è abilitato su una sottointerfaccia ed è un'unità PDU (Bridged Protocol Data Unit) IEEE 802.3, l'incapsulamento Ethernet viene esaminato dopo l'incapsulamento del bridge ATM. Se si tratta di un pacchetto IP/ARP, viene gestito come qualsiasi altro pacchetto IP/ARP. Il pacchetto IP è a commutazione veloce. In caso di errore, viene accodato per la commutazione di processo.

Le prestazioni per il RBE sono un grande successo. Il codice di bridging standard odierno ha il problema intrinseco di richiedere due classificazioni separate per un pacchetto prima che si possa prendere una decisione di inoltro. Una classificazione è definita come il processo di analisi (a monte) e modifica (a valle) dell'intestazione del pacchetto per l'inoltro delle informazioni, che è relativamente costoso. È necessaria una ricerca di layer 2 per determinare se il pacchetto deve essere instradato o sottoposto a bridging. Al layer 3, quindi, è necessaria una ricerca per identificare la posizione verso cui instradare il pacchetto. Questa classificazione viene effettuata nelle direzioni a monte e a valle, con un impatto sulle prestazioni.

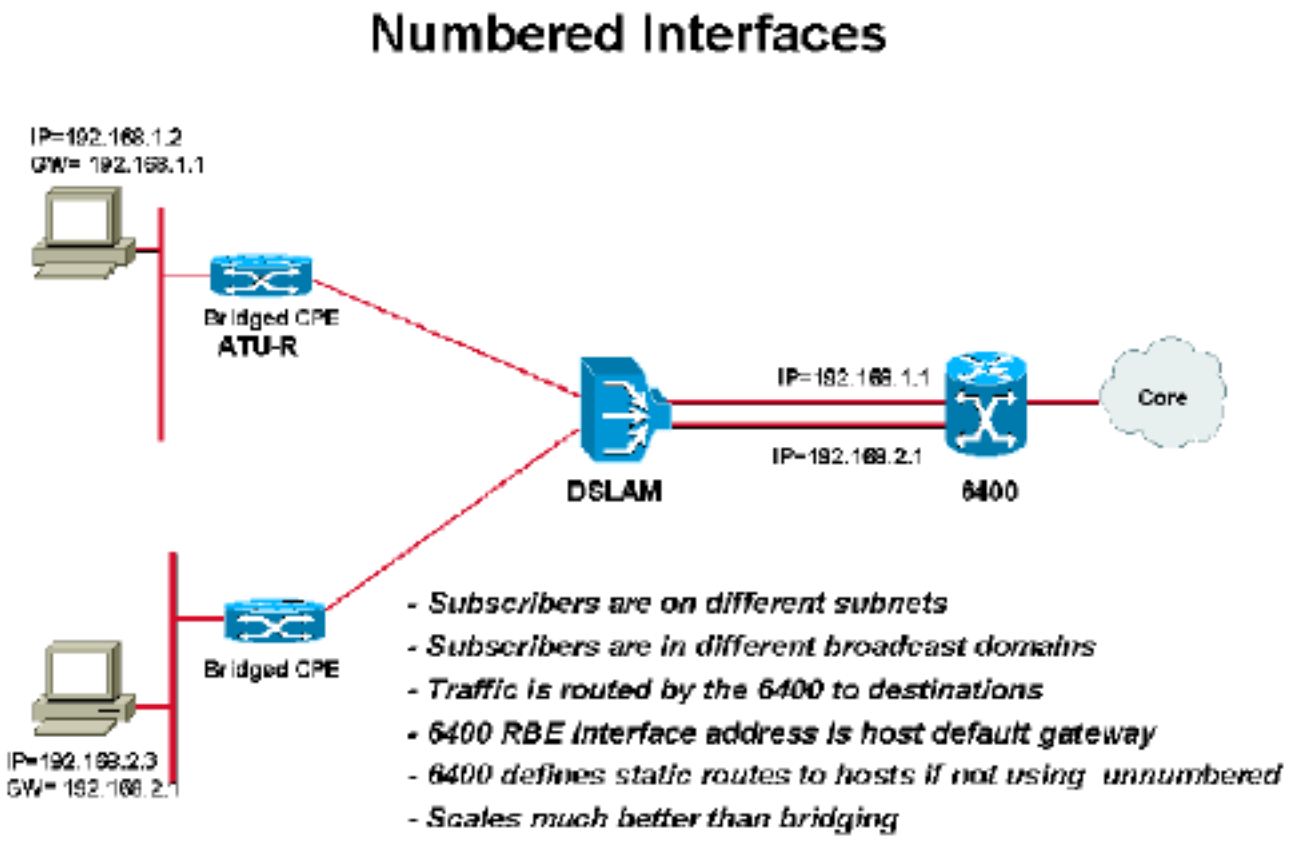
Per il protocollo RBE, è la configurazione che determina il routing del pacchetto nella direzione a monte. Pertanto, non è necessario passare attraverso il percorso di inoltro del bridging, necessario nel caso del bridging standard.

Punti chiave della soluzione RBE

CPE

La configurazione CPE rimane la stessa del bridging standard. Non sono necessarie modifiche al CPE per distribuire RBE.

Gestione IP



Durante la distribuzione delle interfacce numerate per l'interfaccia RBE, l'allocazione degli indirizzi

IP all'host dietro l'interfaccia CPE con bridging viene in genere gestita tramite un server DHCP. Come accennato in precedenza, il server DHCP può risiedere in Protezione accesso alla rete o nell'NSP. In entrambi i casi, la sottointerfaccia ATM numerata deve essere configurata con il comando **ip helper-address**. Se il server DHCP si troverà nell'NSP, il dispositivo di aggregazione di Protezione accesso alla rete deve disporre di una route per raggiungere tale server. L'unico scenario in cui Protezione accesso alla rete utilizzerebbe il proprio server DHCP e il proprio intervallo di indirizzi IP è quando desidera offrire funzionalità di selezione dei servizi ai sottoscrittori, i quali sono LAN collegate a Protezione accesso alla rete.

Se Protezione accesso alla rete desidera utilizzare lo spazio di indirizzi IP dell'NSP, è necessario allocare alla sottointerfaccia ATM uno degli indirizzi IP di ogni subnet. È inoltre necessario che tra Protezione accesso alla rete e Server dei criteri di rete vi sia un accordo reciproco in modo che Protezione accesso alla rete configuri l'indirizzo corretto. Quando il server DHCP del provider di servizi di rete assegna gli indirizzi IP, questo accordo deve essere in vigore per garantire che il server fornisca all'host le informazioni corrette sul gateway predefinito. Protezione accesso alla rete può quindi riepilogare una route statica per tutti gli indirizzi assegnati ai sottoscrittori oppure scegliere di eseguire un protocollo di routing con l'NSP per annunciare tali route. Nella maggior parte dei casi, sia Protezione accesso alla rete che Server dei criteri di rete preferiscono non utilizzare un protocollo di routing. È consigliabile specificare una route statica.

Questa è la configurazione di base richiesta nel NRP per la distribuzione di RBE con interfacce numerate:

```
!
interface ATM0/0/0.132 point-to-point
ip address 192.168.1.1 255.255.255.0
ip helper-address 192.168.3.1
no ip directed-broadcast
atm route-bridged ip
pvc 1/32
encapsulation aal5snap
!
interface ATM0/0/0.133 point-to-point
ip address 192.168.2.1 255.255.255.0
ip helper-address 192.168.3.1
no ip directed-broadcast
atm route-bridged ip
pvc 1/33
encapsulation aal5snap
```

L'utilizzo di interfacce senza numero è il modo migliore per conservare gli indirizzi IP. Come spiegato in precedenza, quando si usano interfacce senza numero con DHCP, le route dell'host vengono installate in modo dinamico. Questo potrebbe essere l'approccio migliore per la distribuzione di RBE. Il server DHCP può quindi trovarsi in Protezione accesso alla rete o nell'NSP, come nel caso delle interfacce numerate.

Questa è la configurazione di base richiesta nel NRP per la distribuzione di RBE con interfacce senza numero:

```
interface Loopback0
ip address 192.168.1.1 255.255.255.0
no ip directed-broadcast
!
interface ATM0/0/0.132 point-to-point
ip unnumbered Loopback0
no ip directed-broadcast
```

```
ATM route-bridged ip
pvc 1/32
encapsulation aal5snap
!
interface ATM0/0/0.133 point-to-point
ip unnumbered Loopback0
no ip directed-broadcast
ATM route-bridged ip
pvc 1/33
encapsulation aal5snap
```

Come raggiungere una destinazione di servizio

Finora in questo documento è stata discussa la tecnologia di accesso di base che utilizza RBE come metodo di incapsulamento. Tuttavia, utilizzando questa architettura, Protezione accesso alla rete/Server dei criteri di rete può anche offrire diversi servizi e diverse opzioni per l'inoltro del traffico degli utenti all'NSP da parte di Protezione accesso alla rete. Questi concetti vengono spiegati nelle sezioni seguenti.

Accesso a Internet

In questo scenario, la funzione principale dell'NSP è fornire agli utenti finali un accesso a Internet ad alta velocità. Poiché l'NSP fornirà il servizio finale, la gestione degli indirizzi IP diventa responsabilità dell'NSP. Può assegnare indirizzi IP pubblici ai suoi abbonati finali utilizzando un server DHCP, o può scegliere di fornire indirizzi IP privati ai sottoscrittori e quindi eseguire NAT per raggiungere il mondo esterno.

Servizi all'ingrosso

Se il PNA intende offrire servizi all'ingrosso ad altri fornitori di servizi internet, può farlo. In questo scenario, Protezione accesso alla rete in genere non preferisce gestire gli indirizzi IP di tutti i sottoscrittori per diversi NSP. Protezione accesso alla rete stabilisce un accordo con l'ISP per fornire indirizzi IP a tali sottoscrittori. A tale scopo, Protezione accesso alla rete inoltra le richieste DHCP provenienti dai sottoscrittori ai server DHCP degli NSP. Protezione accesso alla rete deve configurare le proprie sottointerfacce ATM con uno degli indirizzi IP di tale intervallo e deve annunciare tali percorsi all'NSP. L'annuncio della route potrebbe assumere la forma di una route statica o di un protocollo di routing tra Protezione accesso alla rete e NSP. La route statica è il metodo preferibile per Protezione accesso alla rete e per l'NSP.

Accesso aziendale

L'accesso aziendale richiede in genere servizi VPN (Virtual Private Network). Ciò significa che l'organizzazione non fornirà alcun indirizzo IP a Protezione accesso alla rete e non consentirà a Protezione accesso alla rete di annunciare lo spazio degli indirizzi IP dell'organizzazione nel nucleo IP di Protezione accesso alla rete, in quanto potrebbe causare una violazione della sicurezza. In genere, le aziende preferiscono applicare i propri indirizzi IP ai client oppure consentono l'accesso tramite mezzi protetti, ad esempio Multiprotocol Label Switching/Virtual Private Network (MPLS/VPN) o Layer 2 Tunneling Protocol (L2TP).

L'altro approccio per garantire un accesso sicuro all'azienda è quello in cui Protezione accesso alla rete fornisce gli indirizzi IP iniziali ai sottoscrittori. Pertanto, i sottoscrittori diventano connessi alla rete LAN al Protezione accesso alla rete. Dopo aver ottenuto gli indirizzi IP iniziali, gli abbonati possono avviare un tunnel verso l'azienda attraverso il software client L2TP in esecuzione

sull'host. A sua volta, la società autenticherà il destinatario predefinito e fornirà un indirizzo IP dal relativo spazio di indirizzi IP. Questo indirizzo IP viene utilizzato dalla scheda VPN L2TP. In questo modo, gli abbonati possono scegliere se connettersi al proprio ISP per la connessione a Internet o accedere alla propria società tramite un accesso al tunnel L2TP protetto. Tuttavia, è necessario che l'azienda fornisca l'indirizzo IP di destinazione del tunnel al sottoscrittore, che deve essere instradabile tramite il core IP di Protezione accesso alla rete.

Funzionalità di selezione dei servizi

Protezione accesso alla rete potrebbe offrire diverse funzionalità di selezione dei servizi utilizzando la funzionalità di Cisco SSG. Il SG offre due metodi per fornire la selezione del servizio: tramite PTA-MD (Layer 2) e la selezione Web Layer 3. Con RBE, è possibile utilizzare solo il metodo di selezione Web Layer 3. È quindi necessario che gli abbonati siano connessi alla rete LAN al Protezione accesso alla rete. ovvero, Protezione accesso alla rete fornisce l'indirizzo IP iniziale al sottoscrittore e consente di accedere a Cisco Service Selection Dashboard (SSD).

Nel caso dell'architettura RBE, il metodo di selezione Web di Cisco SSG è un buon metodo per tenere conto del traffico degli utenti.

Conclusioni

RBE offre prestazioni migliori ed è più scalabile del bridging standard. Consente inoltre di superare tutti i problemi di sicurezza che si verificano durante il bridging standard. RBE elimina i problemi di broadcast storm del bridging standard. RBE fornisce un'architettura robusta per Protezione accesso alla rete che desidera evitare la manutenzione del software host del client, risolvere i problemi correlati e ridurre i costi di installazione. Con RBE, tutto questo è possibile utilizzando l'architettura di bridging esistente.

Informazioni correlate

- Informazioni di supporto dei prodotti Cisco ADSL
- Documentazione e supporto tecnico – Cisco Systems